UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
	)	
RYAN HARRIS	)	

DEFENDANT'S PROPOSED PRETRIAL INSTRUCTION

Defendant Ryan Harris, pursuant to Fed.R.Crim.P. 30, submits the following proposed pre-trial instruction to orient the jury to the context and constraints of this case before the trial begins. Apart from this submission, Harris continues to ask this Court to consider his previously filed proposed instructions.

Defendant reserves the right to modify and supplement these instructions as trial progresses.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty
Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on February 14, 2012.

/s/ Charles P. McGinty
Charles P. McGinty

DEFENDANT'S PROPOSED PRE-TRIAL JURY INSTRUCTION

Before you hear from the parties in their opening statements, I want to give you some information and context to help you understand the evidence.

The indictment charges Mr. Harris with wire fraud, and with conspiracy to commit wire fraud, in connection with the sale of cable modem products and services. The government alleges that these products enabled computer users to obtain internet service without making the required payment or to get faster internet service.

I need to make clear what Mr. Harris is not charged with. He is not charged with selling computer modems, or with altering computer modems. It is not a crime to modify or alter a computer modem, nor to sell such a modem, even altered modems that an individual could use to get free or enhanced internet access. Proof that Mr. Harris made or sold altered modems does not alone suffice to establish guilt.[1]

[1] This instruction derives from United States v. Falcone, 311 U.S. 205 (1940) and Direct Sales Co. v. United States, 319 U.S. 703, 710-11 (1943). In Direct Sales, the Supreme Court distinguished the liability of a seller of "articles of free commerce" from that of a seller of restricted goods. Direct Sales, 319 U.S. at 710. The jury must be made aware that the nature of the goods is relevant to its determination of whether Harris had the knowledge and intent necessary to join a conspiracy with TCNISO customers. Id. In those cases, the Supreme Court held that the restricted nature of a product could tend to show that the seller had the knowledge and intent necessary to join a conspiracy with buyers. Id. This holding, combined with the holding in Falcone, clearly indicates that such inferences regarding knowledge and intent cannot be drawn from the nature of an unrestricted product.

I further instruct you that a product's capability alone, that is, whether it can be used for an illegal purpose, cannot support a conviction.[2] Proof that Harris knew that individuals used or could use altered modems to obtain free internet access does not, alone, establish Harris's guilt.[3]

A manufacturer or seller of a product that is legal to make and sell is not liable for the criminal use of that product by an end-user even if the seller knows of the use.[4] Mere knowledge

---

[2] Were this statement not true, manufacturers and distributers of common products, including guns, alcohol, chef's knives, and hammers, could and would face criminal charges based solely on the known capabilities of those products to cause harm. However, even civil liability for such individuals is rare. See, e.g., Perkins v. F.I.E. Corp., 762 F.2d 1250, 1265 n.43 (5th Cir. 1985) ("The marketing of a handgun is not dangerous in and of itself, and when injury occurs, it is not the direct result of the sale itself, but rather the result of actions taken by a third party."). Allowing culpability to rest on capability alone would also have the effect of eliding important elements, including knowledge and intent.

[3] Numerous courts have recognized that product capability alone cannot support criminal liability for a seller. In Direct Sales, the Supreme Court noted that "[a]ll articles of commerce may be put to illegal ends" and warned that "to establish the intent [to join a conspiracy], the evidence of knowledge must be clear, not equivocal," because "charges of conspiracy are not to be made out by piling inference upon inference, thus fashioning what, in [Falcone], was called a dragnet to draw in all substantive crimes." Direct Sales, 319 U.S. at 710-11. As discussed in Harris's motion to dismiss, it has long been accepted law that product capability does not give rise to even civil liability for a seller based on the conduct of product users. George A. Nation, Respondeat Manufacturer, 60 Baylor L. Rev. 155, 157-58 (2008) ("Usually the criminal use of a product is deemed to be a supervening, intervening event that eliminates any responsibility on the part of the manufacturer."); Oliver Wendell Holmes, Privilege, Malice, and Intent, 8 Harv. L. Rev. 1, 10 (1894) (stating that usually vicarious liability for a seller does not exist because "every one has a right to rely upon his fellow-men acting lawfully, and, therefore, is not answerable for himself acting upon the assumption that they will do so, however improbable it may be" (emphasis added)). Nor is suspicion of criminal activity alone sufficient to support a fraud conviction. See United States v. Loder, 23 F.3d 586, 591 (1st Cir. 1994) (in case where defendant's alleged role in mail fraud was helping to dismantle a car, court held that "Although he need not be aware of all the details of the mail fraud, a general suspicion on Loder's part that his participation in dismantling the Caprice was 'for some nefarious purpose' is not enough to make him guilty of aiding and abetting mail fraud.").

[4] "[O]ne does not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally." Direct Sales

of illegal use is not sufficient for conviction. In other words, a seller can be indifferent to a users' purpose, and that indifference does not establish guilt.[5]

Co. v. United States, 319 U.S. 703, 711 (1943).

[5] This instruction is drawn from the Supreme Court opinion in Direct Sales: "[O]ne does not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally." Additionally, in order to be secondarily liable for a crime, one must intend the end of that crime. United States v. Peoni, 100 F.2d 401, 401-02 (2nd Cir. 1938) (holding that accessorial liability requires that the defendant "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed."); see also United States v. Medina-Roman, 376 F.3d 1, 3 (1st Cir. 2004). Here, the targeted, allegedly criminal primary conduct at the base of this indictment is obtaining free or faster internet access. Accordingly, in order to be secondarily liable for someone obtaining free or faster internet access, Harris must have known that the user was planning that conduct and he must have intended to assist them in reaching that end. See United States v. Urciuoli, 513 F.3d 290, 300 (1st Cir. 2008) (holding that in fraud cases, government must prove that defendant willfully participated "in [the] scheme with knowledge of its fraudulent nature and with intent that these illicit objectives be achieved" (internal quotation marks omitted)).

I instruct you that "develop[ing] ... software tools that users could use to steal (or "sniff")" MAC addresses do not constitute fraud. MAC addresses or identifiers are not confidential. Providing the capability to sniff or intercept such addresses is not a fraud on the cable company.

I instruct you that there is no law prohibiting the creation or use of devices, called "sniffers," which can be used to obtain data sent between computers. There is no law prohibiting the use of a sniffer to harvest MAC addresses or configuration files, and there is no law prohibiting sharing these addresses or files with other individuals.[6]

I instruct you that "develop[ing] additional product features that would help users evade detection by ISPs, for example, by disabling the ISP's ability to 'probe' the cable modem to obtain information about it" is not of itself a fraud on the cable company.

I instruct you that uncapping a modem to obtain faster service than you have paid for is not illegal; at most, it may be a violation of the ISP's terms of service.[7]

---

[6] See, e.g., Motion to Dismiss Plaintiff's Consolidated Class Action Complaint, In re Google Inc. Street View Electronics Communications Litigation, No. 5:10-md-02184 JW at 3 (9th Cir. Mar. 21, 2011). Companies including Google, Microsoft, and Apple use this information to help device users pinpoint their location. Id.; see also Leena Rao, Microsoft Taps Navizon to Power Mobile Geolocation, Washington Post, Mar. 2, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030201828.html. Discovery reveals that while investigating Hanshaw, the FBI used a program called Network Stumbler to detect wireless networks in a given area. See Discovery, Bates No. Harris1411-12, Harris1517-18. The FBI used this program on a normal laptop computer running a publicly available Windows operating system. This program detected wireless networks and revealed the MAC addresses of the associated modems to the FBI agent running the program. It appears that the FBI did not have a warrant authorizing the use of this program to reveal MAC addresses and was not otherwise concerned about the legality of this sniffing.

[7] Even the intentional breach of a terms of service agreement cannot be the basis for criminal liability. See United States v. Drew, 259 F.R.D. 449, 466-67 (C.D. Cal. 2009) (holding that intentional violation of MySpace's terms of service–by misrepresenting the identify of the user–could not form basis for conviction under 18 U.S.C. § 1030(a)(2)(C)).

Proof that Harris knew that TCNISO modems could be used to obtain free internet is not sufficient to establish his guilt. Even knowing that a given user might use a device or product to get free internet from a particular ISP is not sufficient to prove guilt. To prove that Harris aided and abetted wire fraud, the government must prove beyond a reasonable doubt that he knew of and intended to help a particular person commit a particular crime; "general suspicion" of wrongdoing is insufficient. United States v. Loder, 23 F.3d 586, 591 (1st Cir. 1994).

Finally, the fact that someone worked for Harris is not proof that Harris was part of a conspiracy with that individual. Agreeing to work with someone to create and sell a product that is legal to create and sell is not proof that those individuals agreed to join a conspiracy to commit wire fraud. The government must prove, beyond a reasonable doubt, that Mr. Harris, himself, knew of and intended to join the charged conspiracy. The fact that someone was Mr. Harris's employee is not proof that Mr. Harris knew of, sanctioned, or is responsible for that individual's actions.